VOLUME 3 GENERAL TECHNICAL ADMINISTRATION

CHAPTER 31 OPERATOR RECORDKEEPING FOR 14 CFR PART 121 AND 135 CERTIFICATE HOLDERS

Section 4 Computer-Based Recordkeeping

3-3051 GENERAL. Many operators are developing computer-based recordkeeping systems, allowing more flexible and efficient maintenance of records. Some computer-based systems offer electronic communications capabilities, which benefit both the operator and the Federal Aviation Administration (FAA). This section contains information and guidance to be used by principal inspectors (PI) when evaluating and approving an operator's computer-based recordkeeping system.

3-3052 REGULATORY REQUIREMENTS. Title 14 of the Code of Federal Regulations (14 CFR) parts 121 and 135 require that operators maintain certain records on crewmembers and aircraft dispatchers. Part 121, § 121.683(c) requires that computer-based recordkeeping systems be approved by the FAA. Part 135, § 135.63 neither specifies the method by which part 135 operator records are kept nor requires approval of computer-based record systems for part 135 operators.

3-3053 GUIDELINES FOR SYSTEM APPROVAL. PIs shall ensure that operators follow certain guidelines and submit certain information when applying for approval of a computer-based recordkeeping system.

A. Approval and Evaluation Process. A part 121 operator may apply for approval of a computer-based recordkeeping system that is designed to satisfy either all regulatory requirements or specific regulatory requirements (SRR), such as training records. When evaluating a computer-based recordkeeping system, PIs shall ensure that the proposed system provides a means of maintaining accurate, timely, and reliable records required by 14 CFR. When approving the system, PIs shall follow the general five-step approval process described in Volume 3, Chapter 1, Section 1. Operations Specification (OpSpec) A025, Electronic Recordkeeping System, is used for the final authorization for an operator's computer-based recordkeeping system.

1) Part 121 operators must apply for approval of computer-based recordkeeping systems by letter.

a) The letter of application must contain the following information:

- A general description of the proposed computer-based recordkeeping system (including the facilities, hardware, and software to be utilized);
- The data backup system to be used;
- Access and security procedures for both the operator and FAA personnel;
- Basic procedures for data entry personnel;
- A general description of any special procedures and capabilities; and
- Electronic signature type(s) and processes to be used.

b) The letter of application must include one or more of the following categories of records, which will be maintained by the computer-based recordkeeping system:

- Crewmember and aircraft dispatcher training records (including pilot, Flight Engineer (FE), flight attendant (F/A), flight instructor, check pilots, check FEs, and aircraft dispatcher training records);
- Aircraft qualification records (including aircraft type ratings, proficiency checks, competency checks, flight checks, and line checks);
- Flight time limitation and rest requirement records;
- Medical qualification records (when applicable);
- Route, "special airport," and area qualification records;
- Operating Experience (OE), consolidation of knowledge and skills, and/or operating familiarization records;
- Pilot recent experience records;
- Check pilot, check FE, and aircrew program designee (APD) designations or authorizations;
- Special training or testing requirements;
- Aircraft listings;
- Load manifests, dispatch/flight releases;
- Communication records; and
- Manual system and revisions.

2) The PI shall ensure that any operator that requests approval of a computer-based recordkeeping system retains data entry forms, or other pertinent nonelectronic records, in a parallel record system. The PI shall ensure that all required records continue to be maintained while the computer-based recordkeeping system is being installed, tested, and evaluated, and data entry personnel are being trained to recognize regulatory terminology and requirements.

B. System Evaluation. PIs shall evaluate the computer-based recordkeeping system capabilities and level of security.

1) Prior to approval, the PI should carefully evaluate the proposed computer-based recordkeeping system to ensure that the system is capable of providing accurate, timely, and reliable records, as required by 14 CFR. The PI shall review the operator's proposed transition plan and user manual, and observe operation of the operator's existing recordkeeping system in parallel operation with the proposed computer-based system. The extent of this evaluation depends on the complexity of the proposed system and its intended use. The evaluation of a system designed to comply with all regulatory requirements will be much more complex than that of a system designed to maintain records in one specific category. The PI shall ensure that system security, record retention periods, and data backups are adequate. Potential problem areas should be identified and corrected prior to approval.

2) PIs shall evaluate the proposed system's level of security to ensure that the database is adequately protected.

a) To maintain the integrity of the database and associated records, the PI should coordinate with the operator during the approval process concerning which FAA personnel will have access to the operator's recordkeeping system. One frequently used approach is to rely on controlled user access codes and passwords.

b) A representative designated by the operator should actively monitor user access and periodically review access control requirements. This representative shall be specifically identified and authorized in the operator's proposal and user manual.

c) A signature may be in the form of a digital signature, a digitized image of a paper signature, a typed notation, an electronic code, or any other unique form of individual identification that can be used as a means of authenticating a record, record entry, or document. The use of electronic signatures enhances the ability to identify a signatory and helps to eliminate the traceability difficulties associated with illegible handwritten entries and the deterioration of paper documentation. The purpose of an electronic signature is identical to that of a handwritten signature or any other form of signature currently accepted by the FAA. The handwritten signature is universally accepted because it has certain qualities and attributes that should be preserved in any electronic signature. Therefore, to be considered acceptable, an electronic signature should possess those qualities and attributes intrinsic to a handwritten signature that guarantee its authenticity.

1. Users of electronic signatures should be aware that not all identifying information found in an electronic system may constitute a signature. Other guarantees commensurate with those of a handwritten signature should be provided. The operator will need to provide verification of an agreement by which it will implement the use of electronic signatures, information interchanges, or alternative methods of information storage. This written agreement means some manner of a recording to memorialize the two parties' agreement. Within the context of this guidance, a written agreement may be part of some other form of document, and it may be a separate instrument.

2. The operator should establish a procedure for allowing designated personnel such as flight instructors, check pilots, check FEs, aircraft dispatcher supervisors, and F/A supervisors to electronically certify all record entries for which they are responsible. This certification may take one of many forms, such as full name, initials, or unique identification number. Each designated person with authorization to make such entries shall be issued a unique individual access code and password in order to validate the entry. The operator may devise a system that requires the validating official to either enter a real-time record into the system or complete a written transmittal document to be given to data entry personnel. If a written transmittal document is used, the identification of the validating official must become part of the record.

3. A computer entry used as a signature should have restricted access that is limited by an authentication code that is changed periodically. The operator should include this in the description of its signature process(es) as approved in OpSpec A025.

4. Any electronic records submitted or maintained in accordance with procedures developed, or electronic signatures, or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form.

d) Appropriate FAA personnel assigned to the operator should be provided with an access level which allows unrestricted data retrieval of all records required by 14 CFR. If the operator elects to use the computer recordkeeping system's capability for electronic designation of APDs, check pilots, and check FEs, an appropriate level of access should be provided to the PI or a designated representative to allow necessary data entries. Any document/information in an electronic format must remain accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

3) The PI shall verify that the operator has established a backup capability to generate a complete set of duplicate records, either electronic or nonelectronic. These records should be stored in a location separate from the main information storage facility. These records may be stored in any form acceptable to the PI, including magnetic tape, magnetic or optical disk, microfiche, or printed records. It should be emphasized that with electronic approval/acceptance of a manual system or revision, no ink signature document is available. For authentication purposes, the approved/accepted material, with the electronic signature attached, must be kept on file for the life of the documents. This will require the carrier and FAA to adopt a reliable, multilayered backup system for the electronic documents. The operator shall back up data as frequently as appropriate to the operator's level of operations and system complexity. For example, a major operator may perform a simultaneous online data backup, while a smaller operator may perform backups at less frequent intervals.

4) The operator shall develop a working procedures manual for day-to-day guidance and training for the operator's employees. This manual should also be provided as a reference document for FAA users. This manual will not require FAA approval but must include guidance in the automated recordkeeping system structure and instructions for using computer commands for such operations as data entry, data processing, data retrieval, and report generation. This manual should address system security procedures and responsibilities, including identification of personnel charged with various levels of data entry, data verification and correction, data audits, and quality control (QC). It should also identify individuals with the authority to issue user access codes and passwords.

5) The PI shall ensure that operators' programs contain audit procedures that are adequate to ensure the accuracy of the database. The frequency and scope of these procedures should reflect the complexity of the computer-based recordkeeping system and the size of the database.

6) Other types of signatures may also be acceptable to the Administrator. An example of an acceptable form of a signature other than a written name is a mechanic's stamp. If a form of identification other than a handwritten signature is used, access to that

identification should be limited to the named individual only. Access to stamps or authentication codes should be limited to the user only. Although a signature may take many forms, the FAA emphasizes that all electronic entries may not necessarily satisfy the criteria that would qualify an electronic entry as an acceptable signature.

3-3054 GRANTING APPROVAL. When all requirements of subparagraphs 3-3053B1) through B5) have been met, the PI may either grant approval for the entire computer-based recordkeeping system or any part of the system. This approval shall be in OpSpec A025 and shall directly reference the manual where the information in the recordkeeping system is maintained.

3-3055 SYSTEM SURVEILLANCE. PIs are responsible for conducting system surveillance, which includes periodic inspections and audits, inspection intervals, and data entry accuracy.

A. Inspections and Audits. After the computer-based recordkeeping system is approved and fully operational, the PI shall ensure compliance through periodic inspections and audits. These inspections and audits shall be conducted using the same criteria as those used during the initial approval process. The PI should plan inspection intervals at least once every 12 months. The annual inspection should normally be conducted in conjunction with National Program Guidelines (NPG).

B. Inspection Intervals. When determining inspection intervals, the PI shall consider the following:

- The size of the database;
- The system's overall sophistication level;
- The extent of the system's security measures; and
- The capability and frequency of the system's self-audit function.

C. Scope of the Inspection. The PI shall determine the scope of the inspection. It may be appropriate to sample a small number of records in each category that the system is approved to maintain, or to conduct an indepth inspection of a specific category of records, such as aircraft dispatcher training.

D. Data Entry Accuracy. The PI shall ensure data entry accuracy during all inspections and audits. A useful evaluation tool might be to compare the operator's required records with FAA surveillance, inspection, and certification records.

3-3056 ADDITIONAL SYSTEM CAPABILITIES. In addition to record retention and retrieval, the operator may request approval of a system with additional capabilities, such as electronic communications and surveillance.

A. Electronic Communications. The operator may provide the PI with email capability, which would allow the operator to request designation of certain airmen, such as check pilots, check FEs, and APDs. This capability would also allow the PI to respond electronically to these requests, thereby increasing both operator and FAA efficiency and convenience. To implement

this email capability, the operator should provide the PI with system access from the PI's facility by providing necessary hardware to be installed at the PI's facility.

B. Electronic Surveillance. The operator may also provide direct access to the operator's computer-based recordkeeping system to allow the PI to carry out required surveillance activities, such as random record retrieval for spot inspections, data audits, selective data retrievals, and reports or summaries. The operator should limit system access to those portions of the recordkeeping system that are used for data retrieval of records required by 14 CFR. Normally, the PI should not be given access to data entry areas; however, the operator may authorize the PI access to data entry areas that pertain to FAA-specific data, such as observations of the pilot in command (PIC), OE, and observation events related to the designation of check pilots, check FEs, or APD candidates.

3-3057 ACCESS TO THE WEB-BASED OPERATIONS SAFETY SYSTEM (WebOPSS).

A. WebOPSS. The FAA provides the aviation industry access to the WebOPSS. Any operator may be given this access through the Internet and through the use of an electronic signature. Current information on this may be found in the OpSpec A025 job aid in association with OpSpec A025 in the WebOPSS Guidance Subsystem.

B. Signature Security. An electronic signature, such as that used in the WebOPSS to sign each OpSpec paragraph, uses electronic approval software and digital certificates using the Public Key Infrastructure (PKI) by a certificate authority (CA). It combines the cryptographic functions of a digital signature and uses a hashing algorithm for authenticating the data, and it provides secure user authentication by permanently referencing a digital certificate within the signature file. These features, among others, make the electronic signatures used in the WebOPSS legally binding and difficult to repudiate.

RESERVED. Paragraphs 3-3058 through 3-3075.